Gabriel Queiroz Lana

Avaliação e Gerência de Confiança Baseada na Maturidade do Usuário em Grades Computacionais

Florianópolis – SC

2008

UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Gabriel Queiroz Lana

AVALIAÇÃO E GERÊNCIA DE CONFIANÇA BASEADA NA MATURIDADE DO USUÁRIO EM GRADES COMPUTACIONAIS

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação

Carlos Becker Westphall

Florianópolis, Fevereiro/2008

AVALIAÇÃO E GERÊNCIA DE CONFIANÇA BASEADA NA MATURIDADE DO USUÁRIO EM GRADES COMPUTACIONAIS

Gabriel Queiroz Lana

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação Área de Concentração de Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

_____

Prof. Dr. Mário Antonio Ribeiro Dantas
Coordenador do Programa de Pós-Graduação em Ciência da Computação

Banca Examinadora

_____

Prof. Dr. Carlos Becker Westphall (Orientador)

_____

Prof. Dr. Mário Antonio Ribeiro Dantas

_____

Prof. Dr. Bruno Richard Schulze

_____

Profa. Dr. Carla Merkle Westphall

AGRADECIMENTO

Ao prof. Westphall, Dr., meu orientador, pela paciência, crédito, conselhos, direções que me apontou e pela oportunidade que me deu junto ao programa de Pós Graduação em Ciência da Computação da Universidade Federal de Santa Catarina. Graças a ele desenvolvi este trabalho.

Agradeço a minha mãe Soraya por ter me apoiado a vir de tão longe para cumprir essa jornada. Ao meu pai Júlio Lana, pelo incentivo e pelas palavras de motivação que me deram força muitas vezes e aos meus irmãos, Túlio e Artur.

A Gabriela, por ter ficado sempre ao meu lado. Pela paciência nas horas difíceis, pela dedicação, pela compreensão e pela estima.

Aos amigos e a todos que passaram e que me ajudaram nessa jornada deixo aqui o meu muito obrigado e a certeza de que valeu a pena.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

P2P	*Peer-to-peer*
CA	*Certification Authority*
TTP	*Trusted Third Party*
ACL	*Access Control List*
ICP	Infraestrutura de Chave Pública
IDS	*Intrusion Detection System*
TM	*Trust Manager*

RESUMO

Gerência de confiança tem sido abordada como um importante fator na segurança de grades computacionais. Grades precisam contar com uma forma segura de confiar em seus usuários sem requerer interações do administrador para tal. Administrar os recursos da grade é uma tarefa que consome tempo. Grande parte do trabalho do administrador pode ser evitado se considerarmos que a maioria das requisições na grade são previsíveis e que dependem apenas do conhecimento sobre o recurso que será utilizado e sobre o requisitante.

Este trabalho irá discorrer sobre gerência de confiança em grades computacionais e sua utilização em ambientes de avaliação para atualizar níveis de confiança. Tratará das diversas formas de definição e conceitos de reputação e confiança, propostas de classificação, métricas para avaliação e modelos de arquitetura de redes de sistema de gerência de confiança. Propõem um modelo de gerência baseado na maturidade do usuário e nas relações de confiança extraídas do curso típico de execução de uma tarefa em grades computacionais. Por estar acima dos *middlewares*, situado no topo da arquitetura, o modelo pode ser incluído para auxiliar sistemas de segurança de grades ao invés de substituir a arquitetura já existente. Pode ser utilizado para fazer recomendações e auxiliar na expedição de autorizações, gerência de recursos e serviços de informação e tomadas de decisão.

Palavras-chaves: Grid; Segurança; Gerência de Confiança.

ABSTRACT

Trust management has been considered an important factor in Grid computing security. Grids require a secure way to establish trust in their participants without requiring continuous intervention by the system administrators. Much of the work of the administrator can be avoided if we consider that the majority of requests in grid are predictable and depend only of the knowledge about the requester and the resource.

This work describes trust management in Grid computing systems and its use in evaluation environments to update the trust levels. It will talk about various forms of definition and concepts of trust and reputation, proposals for classification, metrics for evaluation and models of network architectures of trust management systems. It proposes a model of management based on user maturity and in the trusts relationships that can be obtained in a typical course of task execution in grids. Because it's above middlewares, located at the top of the architecture this approach can be incorporated in Grid security systems to assist in issuing authorisations, in resource and service management, and in decision-making processes.

Key words: Grid computing, security, trust management

1 - INTRODUÇÃO

Apesar de hoje possuirmos computadores domésticos mais poderosos que supercomputadores do passado, a necessidade do aumento de poder computacional continua crescendo. Mapeamento genético, modelagem e simulação científica e de engenharia, diagnósticos médicos e previsão do tempo são alguns de muitos problemas complexos que estão além da nossa capacidade de resolvê-los e que exigem grande quantidade de recursos e hardware de alto desempenho, antes só proporcionados por supercomputadores e clusters de computadores. Porém, essas arquiteturas geralmente possuem altos custos de aquisição e manutenção e em muitos casos não oferecem recursos suficientes para solucionar esses problemas. Roure, Baker, Jennings e Shadbolt mostram em seu artigo *"The evolution of the Grid"* [1] (A Evolução do Grid) como essas abordagens mostraram-se ineficazes e como a evolução dos softwares e hardwares e o barateamento das redes de comunicação fizerem das grades computacionais uma grande solução para problemas que exigem muitos recursos de processamento, armazenamento ou comunicação e que por sua complexidade, não podem ser mantidos num sistema computacional simples administrado localmente e num mesmo domínio [1].

Agregando recursos distribuídos geográfica e administrativamente e provendo alto poder computacional para solucionar problemas complexos e que exigem muitos recursos, a computação em grade ou *grid computing*, surgiu como forma de oferecer recursos mais baratos de forma eficiente em larga escala [2].

Prover segurança nesse ambiente abrange mais variáveis do que aquelas previstas para ambientes mais restritos e controlados. Quando os recursos computacionais estão mantidos e operados localmente, é fácil determinar quem é responsável por autorizar seus usuários e controlar suas ações e solicitações de serviços [3].

Como parte de um sistema geograficamente distribuído, a idéia de se ter uma grade que compartilha recursos traz consigo problemas como violação de informações e estabilidade dos serviços. Dentre outros, tais motivos fazem com que algumas instituições prefiram disponibilizar seus recursos de modo mais fechado, interno e restritivo possível a fim de obter mais segurança em detrimento a flexibilidade e automatizações possibilitadas por tomadas de decisão baseadas em confiança.

Ambientes de grades computacionais podem ter usuários e provedores de recursos em domínios administrativos não confiáveis onde ambos podem agir de modo malicioso [4]. Esse comportamento malicioso geralmente ocorre de duas formas: (1) o programa do usuário pode conter um trecho de código que comprometa a grade ou (2) um nó que possua um recurso compartilhado na grade pode ser malicioso ou estar comprometido prejudicando o resultado esperado pelo usuário que solicitou o serviço [5]. Além disso, diferentes domínios administrativos podem possuir diferentes políticas de segurança sob seus recursos.

O sucesso da computação em grade em ambientes abertos como a internet é altamente dependente de mecanismos de segurança que impeçam violações de informações, garantam autenticidade, autorização, integridade, etc. Assim, a importância das características e modelos de segurança envolvidos nas grades computacionais aumenta na medida em que as grades passam a ser mais utilizadas. Do mesmo modo, o trabalho do administrador também é maior quanto maior for o número de recursos e usuários por ele gerenciados.

Nesse sentido, relações de confiança precisam ser criadas em vários níveis a partir de colaborações entre indivíduos que queiram compartilhar dados, informações ou serviços de forma a obter a menor interação possível do administrador da grade para tomadas de decisão, autorização para utilização de recursos, autenticação de usuários, dentre outros.

1.1 - Caracterização do Problema

A determinação do conjunto de ações que um dado usuário pode executar é fator crucial nos quesitos de segurança das grades. Humphrey em [6] define gerência de confiança como o processo de decisão de quais entidades podem executar quais tarefas. Tomando, por exemplo, a validação do certificado do usuário, isso significa identificar a origem da autoridade certificadora e possíveis atributos e políticas associadas a ele.

Administrar os recursos da grade é uma tarefa que demanda tempo. Esse tempo pode ser reduzido utilizando tomadas de decisão automatizadas, considerando que grande parte do trabalho de administração da grade é previsível e só depende do conhecimento sobre o recurso que será utilizado e sobre o requisitante. O tempo despendido para gerir recursos e usuários em sistemas distribuídos é diretamente proporcional à quantidade desses elementos.

Gerência de confiança e mecanismos de segurança já vem sendo trabalhados há algum tempo e têm sido abordados por diversos pesquisadores [7] [8] [9]. Vários modelos, tais como KeyNote [10], SPKI/SDSI [11], Delegation Logic (DL) [12], SD3 [13] e RT (*Role-based Trust-management Framework*) [14], foram propostos para tornar a computação em grade mais segura, mais flexível e mais abrangente.

Em sistemas de grades, confiança geralmente é construída e mantida em conjunto com mecanismos de segurança. Em [15], Lin descreve que muitos modelos são especialistas e tratam pontualmente da utilização de confiança para aprimorar alocação de recursos nos sistemas de grades computacionais e propõe um modelo formal e genérico que captura as relações de confiança na grade e provê mecanismo para avaliação e atualização dinâmicas da confiança para auxiliar na tomada de decisões.

Mecanismos de autenticação baseados em certificados garantem que um usuário pertence a uma organização confiável e que utiliza ou disponibiliza recursos na grade de maneira previamente acordada. Um novo nó pode ser inserido e aceito como participante desde que ele concorde com os requisitos impostos pela autoridade certificadora e a autoridade certificadora concorde em emitir certificados para esse novo nó. Para isso, faz-se necessário uma interação humana nesse processo [16].

Sistemas de grades contemplam grande quantidade de nós e por sua característica ubíqua, precisam de um meio para manter e disponibilizar a reputação de qualquer entidade a partir do momento que ela passa a participar da grade. Tal asserção é justificada por referir-se a entidades que podem pertencer a qualquer organização ou a entidades ditas voluntárias, que disponibilizam um serviço apenas por um determinado período ou simplesmente participam da grade por pouco tempo.

Após um estudo aprofundado e abordagem dos tipos de métricas para avaliação de confiança, este trabalho propõe uma nova forma para avaliar e gerir os níveis de confiança de um modo genérico baseando-se nas relações de confiança que podem ser extraídas do curso típico de execução de uma tarefa em grades e do espalhamento e atualização dos níveis de confiança através de gerentes de confiança.

1.2 - Objetivos do Trabalho

Este trabalho tem como objetivo geral propor uma nova forma de medir confiança e gerenciar reputação em sistemas de grades computacionais.

1.2.1 - Objetivos Específicos deste trabalho são os seguintes:

- Estudo dos conceitos e definições de confiança a fim de identificar relações entre elas e contribuir para o estabelecimento de um senso comum;
- Rever e discutir as recentes pesquisas na área de gerência de confiança e reputação; e,
- Identificar propriedades e características positivas e negativas das diversas abordagens e propor melhorias e soluções.

1.3 - Trabalhos Correlatos

Diversos sistemas de confiança foram propostos em pesquisas nas áreas de gerência e segurança. Tais sistemas contemplam basicamente dois problemas [17].

O primeiro é o problema da modelagem semântica de dados, como gerar, interpretar e avaliar medidas de confiança e reputação. O segundo problema é do gerenciamento dos dados, ou seja, como armazenar, recuperar, distribuir e garantir que são seguras, as informações sobre medidas de confiança e reputação, de modo escalável e eficiente.

EigenTrust [18] [19] é um algoritmo de gerência de reputação para redes *peer-to-peer* (P2P). Ele garante um valor de reputação para cada entidade (*peer*) baseado no resultado das últimas interações. Os valores de confiança são computados localmente. Para melhorar o desempenho, o processo de cálculo do valor de confiança global é realizado com um conjunto de entidades vizinhas. A segurança é garantida fazendo com que os valores de confiança não sejam armazenados pelas partes interessadas, mas sim por outras entidades da rede selecionadas através de um mecanismo subjacente de roteamento.

O Grid EigenTrust [20] surgiu baseado no Eigentrust para suprir limitações deste modelo quando aplicando em grades computacionais. Os autores citam, entre outros, três pontos importantes que foram reestruturados e deram origem ao Grid EigenTrust. Primeiro, o EigenTrust foi claramente criado para redes P2P e diversos termos utilizados não são adequados ao contexto de grades. Segundo, os autores também argumentam que a medida de confiança entre entidades vizinhas não representa um valor de confiança global e tal cálculo para muitas organizações seria demasiadamente custoso, pois teria que considerar todas as relações entre todas as entidades. E terceiro, o EigenTrust foi estudado somente nos contextos de armazenamento, impressão e processamento e grades contemplam muito mais recursos. O EigenTrust utiliza uma função que reduz o valor da confiança baseada no tempo de interação. Por não considerar a grande diversidade de serviços providos em grades, não se observou, por

exemplo, que em uma transmissão de arquivo demorada, tal função poderia invalidar a reputação antes mesmo de a transferência ser concluída.

Xiong e Liu apresentaram o sistema chamado PeerTrust [21]. O sistema utiliza cinco parâmetros combinados em uma equação genérica para medir a confiança. Os parâmetros são *feedbacks* de outros *peers*, freqüência das transações, credibilidade dos *feedbacks*, o contexto da transação e contexto da comunidade. Cada *peer* armazena uma parte dos dados globais de confiança e um *peer* gerente monitora e avalia a confiança dos outros *peers*. Para isso, utiliza replicação, criptografia e possui uma robusta infra-estrutura de roteamento necessária para organização dos *peers* e da informação de confiança neles distribuídos.

Em [4], Lin et al apresenta uma arquitetura de gerência de confiança para sistemas de segurança de grades computacionais baseada em lógica subjetiva. Possui tomada de decisões baseadas em medidas de confiança para aprimorar os sistemas de segurança de grades computacionais. Os autores também incorporam um sistema de autorização baseado em confiança para ser incorporado à tradicional abordagem baseada em políticas. Além disso, apresentam um protocolo de recomendação, análises de requisições de tarefa baseada em confiança, atualização baseada no conhecimento presente e passado do comportamento da entidade e avaliação do nível de confiança utilizando noções de experiências positivas e negativas.

Quillinan et al desenvolveram o GridAdmin [22], um sistema para automatizar tarefas típicas de administração em grades tais como reserva de recursos e gerenciamento de contas de usuários. Foi proposta uma métrica de avaliação de confiança baseada em lógica difusa e implementada dentro do *middleware* WebCom [22]. A utilização de lógica difusa aproxima o significado de confiança da forma como costumamos tratá-lo no dia a dia.

Também com lógica difusa, Song e Hwang sugerem melhorar o nível de segurança atualizando os sistemas de defesa contra intrusão baseado em *hosts* e verificando o sucesso de tarefas executadas em suas plataformas [9]. O modelo também prevê atualização do nível de confiança, propagação dessa informação e integração entre os sites. Com lógica difusa, o modelo é capaz de qualificar dados imprecisos ou incertos a fim de mensurar o nível de segurança dos sites.

Guha et al estudaram a propagação de confiança e desconfiança [23]. Em seu trabalho, foram os primeiros a propor um modelo formal de um esquema de propagação de confiabilidade onde introduzem um tratamento formal e computacional de desconfiança. Também desenvolveram um tratamento para contornar o problema de decidir se uma entidade *i* deve confiar em outra entidade *J* quando utilizam valores contínuos de confiança ao invés de utilizar valores discretos como na maioria dos trabalhos. Tal tratamento inclui três formas de contornar o problema. Ele utiliza comparação global, local ou predição pela maioria da relação dos valores de confiança e desconfiança das outras entidades.

Walsh e Gun [24] introduzem a noção de reputação de objetos. Para combater o que eles chamam de poluição nas redes *peer-to-peer*, os autores desenvolveram um modelo para prover estimativas confiáveis sobre a autenticidade de um objeto e fornecem incentivos para que os nós contribuam e avaliem honestamente os objetos compartilhados, denunciando-os como maliciosos ou *spam*. Tipicamente, quando faltam evidências para afirmar que um objeto é inválido ou não confiável na rede, os nós utilizam um indicador *ad hoc* de reputação de objetos baseados num esquema de estatísticas de correlações entre nós, com base em saber se as avaliações dos nós para um mesmo objeto concordam ou discordam entre si e assim, formando uma matriz de correlação.

1.4 - Organização do Trabalho

A organização do trabalho será disposta da seguinte forma: A seção 1 descreveu a gerência de confiança e sua importância no ambiente de grades. A seção 2 irá discorrer das definições e conceitos envolvidos e das abordagens de classes de confiança. A seção 3 tratará das métricas para cálculo de confiança e de onde pode ser obtidas relações de confiança no ambiente de grades baseando-se no curso típico de requisição/execução de uma tarefa. O quarto tópico expõe as arquiteturas de rede centralizada e distribuída dos sistemas de gerência de confiança e propõe um modelo distribuído para interação entre gerentes de confiança. O quinto item apresenta e descreve a metodologia para avaliação

da confiança baseada na maturidade do usuário e explica os diversos parâmetros propostos. A seção 6 relata as interações entre os gerentes de confiança. Por fim, o item 7 conclui sobre as contribuições do trabalho e aponta os trabalhos futuros.

2 - CONFIANÇA E SEGURANÇA

Confiança e segurança são duas áreas ligeiramente distintas em grades computacionais. Muhammad e Yuanda [25] enfatizam que infelizmente algumas vezes gerência de confiança é confundida com infra-estrutura de chaves públicas (ICP). Eles destacam que modelos de confiança em ICPs ou Listas de Controle de Acesso (ACL – do inglês, A*ccess Control List*. Optou-se por manter a sigla em inglês por esta ser mais difundida),são chamadas modelos de confiança objetivos onde os objetos especificam restritas relações de confiança entre as entidades. Tais modelos consomem recursos demasiadamente e não provêem a flexibilidade esperada. Além disso, em caso de falha eles afetam toda a estrutura dependente e os danos podem ser irreparáveis.

Essa última consideração fez com que a confiança subjetiva, da forma como costumamos utilizá-la no dia a dia, ganhasse espaço num meio onde só se utilizava confiança objetiva.

Ainda hoje, os atuais trabalhos sobre gerência de confiança divergem sobre o a polêmica levantada em [25]. Muitos trabalhos desconhecem ou desconsideram a afirmação sobre a confusão das abordagens.

Este capítulo visa esclarecer e exemplificar com diversas definições de confiança como os conceitos são utilizados e agrupá-los numa definição média para auxiliar no senso comum.

2.1 - Confiança em Grades Computacionais

Confiança é um termo complexo que envolve a crença na veracidade, honestidade, competência e diversas características subjetivas relativas ao caráter de entidades. Em grades, essas entidades são todos componentes envolvidos em uma operação que podem se relacionar uns com os outros estabelecendo alguma relação de confiança. Podem ser desde nós provedores de recursos e usuários até terceiros, também envolvidos no

processo, tais como sistemas gerenciadores de recursos e autoridades certificadoras (as CAs – do inglês, *Certification Authority*).

2.2 - Conceitos e Definições

Azzedin e Maheswaran em [26] definem confiança como sendo a crença na competência de uma entidade em agir da forma prevista e esta crença não é um valor fixo, mas sim um valor sujeito ao comportamento da entidade e que se aplica apenas dentro de um contexto específico e em um determinado tempo.

Em sistemas de tomadas de decisão baseados em confiança, é fácil associar que uma entidade é confiável considerando seu histórico. Nesses sistemas, uma entidade pode confiar em outra para obter informações relativas a outras entidades e que sendo assim, reputação é encontrar meios de confiar em uma entidade [25]. Em [25], Muhammad e Yuanda definem reputação como sendo a expectativa do comportamento de uma entidade baseando-se em seu comportamento passado obtido através de observações e informações fornecidas por outras entidades.

Ainda há uma ressalva onde, fortuitamente, há um consenso sobre as características de relações de confiança de um modo geral e que elas são aplicáveis ao contexto de grades computacionais. Relações de confiança podem ser de um pra um, um para muitos, muitos para muitos e muitos para um, não são transitivas e a confiança é dinâmica e atrelada ao tempo [25].

Segundo Christianson e Harbison em [27] deve-se desconsiderar o conceito de transitividade visto que uma entidade B que se relaciona com uma entidade A para prover-lhe algum tipo de serviço pode agregar relações de confianças com outras entidades sem o consentimento explícito de A, resultando no que os autores chamam de transitividade sem intenção. Em outras palavras, B confia e estabelece relações de confiança com entidades que A desconhece, não confia ou confia pouco. Apesar de a transitividade de confiança poder causar resultados inesperados e adversos, há autores que a consideram necessária em alguns casos. Grandison e Sloman [28] explicam que a transitividade herdada de algumas relações de confiança deve ser considerada nas análises de sistemas de confiança para determinar e prevenir efeitos inesperados.

A idéia por trás da transitividade é que quando uma entidade A confia em B, B confia em C e B refere-se a C para A, então A pode estimar uma medida de confiança em C combinada com a confiança que ela possui em B. Essa transitividade é ilustrada na figura a seguir que foi traduzida de [29].

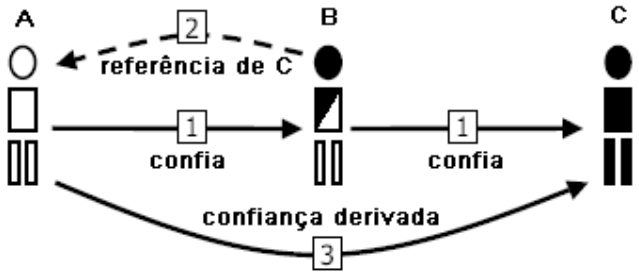

Figura 1 - Princípio da transitividade de confiança

Muitos trabalhos sobre confiança e gerência de confiança no contexto de grades computacionais, sistemas *peer-to-peer* e sistemas distribuídos trabalharam na definição e no significado de confiança. Uma importante e influente definição de confiança foi dada por [30] da seguinte forma: Quando dizemos que confiamos em alguém ou que alguém é confiável, nós implicitamente atribuímos que a probabilidade que essa entidade confiável vá executar uma ação benéfica ou pelo menos não prejudicial é grande o suficiente para cooperarmos um com o outro. De modo correspondente, quando dizemos que uma entidade não é confiável, implicamos que a probabilidade é baixa o suficiente para não cooperarmos. Gambetta escreve enfaticamente que confiança é fundamentalmente uma crença ou uma estimação e que esse modo de analisar a confiança inspirou o uso de lógica subjetiva como forma de medição [31].

Kini e Choobineh [32] incluíram diversas características humanas de confiança abordando o tema de perspectivas como a teoria da personalidade, sociologia, economia e psicologia social. Eles definem confiança de acordo com o dicionário Webster [51]. Apesar de suas análises abrangerem elementos humanos de confiança em sistemas computacionais, eles não avaliaram a confiança entre entidades envolvidas em transações de comércio eletrônico. A principal contribuição foi o detalhamento das implicações dessas definições e a combinação de seus resultados para criar uma definição de confiança em um sistema computacional. Eles definiram confiança como

sendo a crença que é influenciada pela opinião do indivíduo acerca das características críticas do sistema.

Grandison e Sloman [28] contemplam várias definições de confiança. Em seu trabalho, definem confiança como a firme convicção na competência de uma entidade em agir de forma segura e confiável dentro de um determinado contexto. A argumentação importante desse trabalho é que confiança é não só a composição de diversos atributos como fiabilidade, confiabilidade, honestidade, veracidade, segurança, competência e atualidade, mas também a sua consideração e definição em um ambiente específico de confiança.

Além disso, afirmaram que desconfiança (*Distrust*) pode ser um conceito útil como forma de desfazer acordos de confiança previamente estabelecidos ou em ambientes onde as entidades, por padrão, são confiáveis e é necessário identificar aquelas que não são confiáveis.

Dimitrakos [33] define confiança da seguinte forma: A confiança de uma *parte* A numa *parte* B para um *serviço* X é a crença mensurável de A na *denpendabilidade* do comportamento de B para um *período* específico e dentro de um *contexto* específico em relação a X. No contexto de sua definição, o termo “parte” é entendido como entidade, um conjunto de pessoas ou processos, ou um sistema; “serviço” é utilizado de forma ampla a fim de incluir transações, recomendações, emissão de certificados, etc; da mesma forma, “dependabilidade” também é um conceito lato e engloba segurança, confiabilidade, atualidade e durabilidade; “período”, que pode ser a duração do serviço, refere-se ao passado, futuro (*slots* de tempo críticos agendados ou previstos), ou sempre; e por fim, “contexto” refere-se a relevantes acordos de serviços, histórico de serviços, infra-estrutura tecnológica, *frameworks* legislativos e regulatórios que pode ser utilizados.

Jøsang et al [29] definem confiança como a medida de quanto uma entidade está disposta a depender de algo ou alguém com sentimento de relativa confiança numa dada situação, mesmo que isso possa ter conseqüências negativas. Em sua argumentação, os autores falam de aspectos como dependência de entidades confiáveis, conceito de utilidade no sentido de que uma informação verídica dita de utilidade positiva provém de resultados positivos e utilidade negativa provém de resultados negativos e também falam sobre atitude de risco.

Há pouco mais de uma década, quando o conceito começou a ser discutido, ainda não existia nenhum consenso sobre a definição de confiança [34], mas já era visto como um importante requisito que deveria ser tratado no futuro e que envolvia honestidade, veracidade, competência e segurança, entre pessoas ou serviços. Atualmente as definições possuem diversos pontos comuns e muitas são complementares. É notável que em diversas concepções confiança possua caráter subjetivo, inerente às características humanas de confiança, como em [28] [33] e [29].

Em [28] ainda encontra-se que uma entidade confia em outra para um específico negócio ou serviço, incluindo na definição particularidades de aplicações baseadas na Internet.

E por fim, [33] destaca um ponto importante: confiança está atrelada ao tempo e é mensurável.

Até aqui, vimos importantes definições de confiança e características importantes que precisam ser levadas em conta. Nos capítulos que se seguem, confiança deve ser interpretada como algo mensurável relativo a capacidade, competência e fé em outra entidade em prover ou utilizar algum serviço específico em um determinado momento de maneira benéfica ou ao menos não prejudicial. Já reputação, é relativa ao histórico do comportamento passado e explícito (ou identificado por IDSs, por exemplo) de uma entidade ao utilizar ou prover determinado serviço. Esse histórico pode ser avaliado por experiências próprias, ou seja, iterações e cooperações passadas com a entidade em que se pretende confiar, e pode ser utilizado em conjunto com opiniões ou recomendações de terceiros que já estabeleceram relações de confiança com a entidade que se pretende confiar ou receberam recomendações sobre ela.

2.3 - Classes de Confiança

Lin et al[4] analisaram o curso típico de requisição e execução de uma tarefa em um sistema de grades para mostrar de onde podem ser extraídas as relações de confiança. Para isso, eles formularam uma série de questionamentos divididos em três momentos desse curso que estão dispostos a seguir.

No primeiro momento, antes de enviar a requisição a um nó provedor do recurso, o usuário precisa saber se o provedor do recurso será capaz de realizar a tarefa e se ele

pode confiar nessa execução. Isso é chamado confiança de execução. Em seguida o requisitante precisa saber se o provedor do recurso confia suficientemente nele para cooperarem entre si. Ainda no primeiro momento, o usuário precisa ter certeza que o provedor não alterará o código ou o resultado da computação.

Antes de executar a tarefa no nodo provedor do recurso, o segundo momento deve considerar duas questões relativas a confiança no código: o usuário precisa ser capaz de produzir códigos que não prejudicarão a grade, ou de modo mais agressivo, o provedor do recurso precisa confiar que o usuário não enviou um código malicioso ou requisitou uma tarefa que possa comprometer o sistema. A outra questão é: o programa do usuário foi alterado antes de ser alocado?

Por fim, no terceiro momento, após a conclusão e resultado da tarefa, o usuário precisa checar a integridade dos resultados e atualizar a confiança de execução para o provedor do recurso, que por sua vez deve atualizar sua confiança de código para aquele usuário.

Com base no curso típico de execução de uma tarefa em grades computacionais, Lin et al classificam e definem as relações de confiança em cinco tipos: de autenticação, de execução; de código; direta; e confiança recomendada [4].

Confiança de Autenticação: Confiança de autenticação é a crença na autenticidade de uma identidade assinada por uma autoridade certificadora chamada TTP (*Trusted Third Party*) para um participante da grade.

Confiança de Execução: Confiança de execução é crença que um nó provedor de recurso executará fielmente o código do usuário e/ou completará a tarefa solicitada.

Confiança de Código: Confiança de código é a crença que um nó provedor de recurso possui num usuário em relação a sua capacidade e competência em produzir códigos seguros e que não prejudicarão a grade.

Confiança Direta: Confiança direta é a crença que uma entidade possui na capacidade, benevolência e relevância de outra entidade numa determinada classe de confiança.

Confiança Recomendada: Confiança recomendada expressa a crença na capacidade da entidade decidir se outra é confiável quando esta a recomenda confiar em uma terceira entidade em uma dada classe de confiança.

Grandison e Sloman [28] classificam confiança em cinco diferentes classes: provisão de serviços; acesso a recursos; delegação; certificação; e infra-estrutura.

A figura a seguir, baseada em [29], representa as classes de confiança de Grandison e Sloman [28]. A união de todas as classes converge para Finalidade de Confiança [51], um conceito global que pode ser utilizado para expressar qualquer instanciação operacional de qualquer uma das classes, ou seja, serve para definir o escopo das relações de confiança.

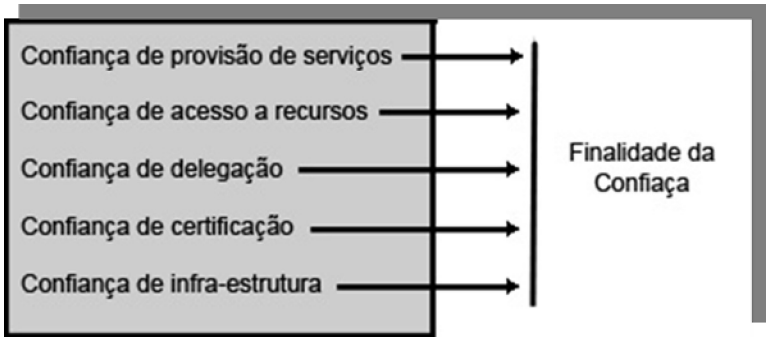

Figura 2 - Classes de confiança de Grandison e Sloman [28]

- **Confiança de provisão de serviços** descreve a parte de confiança relacionada aos recursos e serviços, isto é, quando um usuário precisa confiar no provedor do recurso. Essa confiança vem antes da utilização efetiva do recurso, isto é, a entidade utilizadora confia no provedor do recurso independentemente da forma como ele o provê (utilizando terceiros ou não, por exemplo), mas sob uma determinada pré-condição. Por exemplo, uma entidade A só contrata os serviços de armazenamento de B, caso B, entidade provedora do recurso, pertença à empresa XYZ, independente de a entidade provedora contratar recursos de terceiros para fazê-lo.
- **Confiança de acesso** a recursos refere-se à relação entre uma entidade que acessa os recursos em outra entidade é dona ou responsável pelo recurso provido. Considera-se ainda, que é tipicamente controle de acesso e foi o principal foco de pesquisas em segurança durante várias décadas [35] e é considerado um elemento central em segurança computacional. Este tipo de

confiança pode ser mais detalhado se considerarmos políticas de autorização que definam as ações permitidas pela entidade utilizadora do recurso durante o acesso. Tais permissões podem incluir tempo de acesso, permissões de escrita e leitura, quantidade de espaço em disco ou utilização de memória. Nesse contexto, há uma clara distinção entre confiar em uma entidade que vai apenas ler ou gravar um arquivo no servidor e uma entidade que vai executar algum código [28]. Acesso a arquivos implica somente em seguir corretamente o protocolo utilizado para transferência, não divulgar informações, ler e gravar somente dados permitidos. Execução de código requer um nível maior de confiança visto que um código malicioso pode danificar o provedor do recurso ou, se em maiores proporções, até toda a grade. Além disso, precisa-se considerar ainda, limites como quantidade de memória utilizada, processamento e que a execução termine em um tempo finito.

- **Confiança de delegação** pode ser descrita como a confiança que uma entidade provedora do recurso possui numa outra entidade que toma decisões por ela [36]. A delegação, na maioria das implementações, é utilizada no controle de acesso. Ding e Petersen [36] conceberam um sistema de delegação hierárquico baseado em tokens. A delegação diminui a carga de tarefas do provedor do recurso, mas é preciso haver políticas para restringir o uso de delegação e a redelegação.

  Existem três formas de redelegação:

  - Sem controle, o que significa que qualquer permissão pode ser redelegada. Está é a abordagem utilizada em [10], porém ela contradiz o conceito de não transitividade de confiança e por isso a maioria dos sistemas de gerenciamento de confiança não a utilizam;
  - Com controle booleano, utilizado em [11], provê a capacidade de especificar a incapacidade de redelegação;
  - E com controle inteiro, no qual é possível especificar um valor inteiro para a profundidade de redelegação. Em [12], há uma interessante abordagem desse método, a qual permite especificar

a profundidade por um inteiro positivo ou por um "*", que permite redelegações ilimitadas;

- **Confiança de certificação**, também chamada de "*authentication trust*" [37] ou de "*identity trust*" [29], representa a confiança que a entidade provedora possui no certificado apresentado pela entidade que requer o recurso. Esquemas de confiança de certificação são tipicamente sistemas de autenticação, como X.509 [52] [53], PGP [54] e [55]. A autoridade certificadora provê o serviço de validar a veracidade de uma entidade por meio do serviço de certificação o que torna confiança de certificação um forma especifica de confiança de provisão de serviços, mas envolve um terceiro para estabelecer a confiança [29].
- **Confiança de Infra-estrutura**, também conhecida como "*context trust*" [29] e "*system trust*" [34], refere-se a confiança que a entidade provedora do recurso precisa ter em na sua infra-estrutura base. O provedor do recurso precisa confiar nele mesmo, ou seja, no seu próprio hardware incluindo sua rede local e servidores locais os quais pode implementar alguma segurança ou outro serviço para proteger sua infra-estrutura. [29] vai mais além e considera sistemas, instituições e todo o contexto necessário para suportar transações e prover segurança caso algo dê errado.

3 - AVALIAÇÃO DE CONFIANÇA

A confiança deve ser mútua entre o *host* e o provedor do recurso. Mas como estabelecer um nível de confiança nas relações envolvendo essas entidades? E como avaliar a confiança? Basicamente, as métricas atualmente utilizadas nessa relação podem ser divididas em dois tipos: métricas baseadas na reputação do usuário e métricas financeiras, baseadas na "compra" de recursos.

Técnicas de medidas baseadas em reputação já foram muito estudadas e estão muito bem estabelecidas atualmente como forma de avaliar o nível de confiança [18] [21] [38]. Nessa abordagem, manter e obter a medida de reputação do usuário permite que o administrador possa tomar decisões sobre, por exemplo, alocação de recursos para esse usuário ou negação de algum serviço. Essa medida é chamada de karma. O karma é um valor numérico, reflexo do comportamento passado, que representa o nível de confiança do usuário em um determinado sistema local. Valores altos indicam um usuário confiável. Dessa forma é possível tomar decisões automáticas para determinados níveis de confiança.

A dificuldade dessa técnica é administrar e atualizar os valores dos karmas, já que esses, na maior parte das implementações, ficam nas credenciais dos usuários. Essa necessidade é suprida de vários modos. Um deles é utilizando uma data de expiração do karma que pode ser adicionada à credencial, forçando o usuário a obter novas credenciais periodicamente quando o karma estiver vencido. A desvantagem dessa solução é o custo computacional extra na revalidação dos certificados dos usuários. O modelo, a ser descrito em seguida, soluciona esse problema com a adoção dos gerentes de confiança de domínio e com a atualização e propagação da informação entre os gerentes conhecidos.

Um ponto importante a ser ressaltado nessa abordagem, é a atribuição do valor inicial do karma do usuário. Como avaliar a reputação de um usuário que não possui histórico? O modelo de avaliação de confiança baseado na maturidade do usuário exposto a seguir soluciona esse problema.

As métricas financeiras são baseadas em trocas de moedas padronizadas entre os participantes. O sistema funciona basicamente da seguinte forma: para utilizar um recurso, um valor acordado previamente deve ser pago ao dono do recurso e esse valor é reembolsado futuramente. Em sistemas de troca mais fechados, a moeda pode se tornar cupons de troca, no qual o possuidor os cede para utilizar um recurso e quando provê algum recurso os obtém de volta. A grande vantagem dessa abordagem é que ela implica em baixa computação e baixo custo de administração, porém pode causar *dead-locks* caso algum usuário poupe cupons por muito tempo.

Em métricas financeiras, idealmente um usuário pode economizar dinheiro ou um conjunto de usuários podem se organizar a fim de utilizar um recurso mais caro. Maus comportamentos, como, por exemplo, monopólio de cupons de troca, são desencorajados retirando-se moedas do usuário quando ele efetuar transações.

Os modelos atuais que utilizam métricas baseadas em reputação são claramente mais adequados a sistemas de grades pequenos devido às suas características peculiares a cada sistema e por não preverem nenhum tipo de atualização, propagação nem de troca de informações entre domínio com diferentes administrações, enquanto métricas financeiras são mais utilizadas em sistemas de grades mais amplos e com interações entre domínios diferentes, caso típico de organização virtual.

Nesse contexto, este trabalho sugere introduzir esquema de critério de avaliação de confiança baseado em níveis de maturidade do usuário com progressões definidas e previamente coordenadas e estabelecidas pelo administrador da grade onde é utilizada uma premiação ao usuário que faz bom uso do recurso. Além da premiação, o esquema propõe uma forma para avaliação da confiança de usuários provenientes de outros domínios administrativos, utilizando comunicação entre gerentes de confiança.

Com o sistema baseado na maturidade do usuário, este trabalho introduz um novo modelo de avaliação de confiança que pode ser tão desejado para sistemas pequenos e mais restritos quanto para grandes organizações virtuais. Além disso, o esquema é independente de outros métodos podendo inclusive ser utilizado em conjunto com outras técnicas para avaliação de confiança.

3.1 - Cálculo de Confiança e Reputação

O cálculo da reputação pode ser realizado com base nas informações adquiridas a partir de experiências próprias, por recomendações ou por uma combinação dessas duas origens. Aqui pode-se discernir dois tipos de confiança: confiança direta e confiança recomendada.

Um problema aqui é como avaliar as recomendações. Os sistemas de avaliação de confiança precisam decidir quão importante é uma recomendação, se ela pode ou não ser repassada e como ela deve ser repassada.

Sistemas de reputação são tipicamente baseados em informações providas por outras entidades de modo a representar a opinião da comunidade [29]. Também é fácil perceber que uma entidade que confia na reputação de outra está na verdade confiando através da característica de transitividade da confiança. Por exemplo, sejam três entidades A, B e C, podemos dizer que A confia em B porque C forneceu uma informação a A sobre a boa reputação de B e A já confiava em C.

Os valores de confiança podem ser valores discretos, por exemplo, de um a cinco, onde um representa totalmente não confiável, dois, pouco confiável, três, confiável, quatro, muito confiável e cinco, totalmente confiável, como proposto em [47], ou podem ser valores contínuos, onde não há uma faixa de valores predefinida e o valor da reputação é acrescido ou subtraído de acordo com o comportamento da entidade.

O modo mais simples de se calcular reputação através dos diversos valores de confiança é por meio de uma média aritmética simples, no caso de valores discretos, e cômputo separado dos valores positivos e negativos e totalização desses valores através de uma simples subtração dos valores negativos dos positivos, no caso de valores contínuos,

Os websites Epinions [56] e Amazon [57] utilizam média aritmética simples. No caso de valores contínuos, os *web sites* de leilão Ebay [58] e Mercado Livre [59] são importantes exemplos. A vantagem desse método é o baixo custo computacional do cálculo da reputação e sua simplicidade em si, pois qualquer usuário é capaz de compreender como a reputação é calculada. A desvantagem é que ele traz um retrato pobre da reputação do usuário.

Implementações de cálculos de reputação envolvendo inferência bayesiana são bastante utilizados quando se trata de modelos probabilísticos para avaliar confiança [40] [41] [42] [43] [44] [45].

Inferência bayesiana é um método estatístico baseado no teorema de Bayes que considera fundamental na estatística a informação que se tem sobre uma quantidade de interesse desconhecida θ. A idéia é tentar reduzir esse desconhecimento. Assim, existem diferentes graus de incerteza representados por meio de modelos probabilísticos para θ oriundos de diversas propostas de pesquisadores. A informação que temos de θ pode ser resumida probabilisticamente por

$$p(\theta) \quad (1)$$

(probabilidade *a priori*) e pode ser mais próxima do valor real quanto maior for uma amostra de quantidade X.

$$p(x|\theta) \quad (2)$$

representa a plausividade ou verossimilhança de um valor fixo da amostra X em relação a probabilidade θ anterior. Usualmente, tem-se o teorema de Bayes da seguinte forma:

$$p(\theta|x) \propto p(x|\theta)\, p(\theta) \quad (3)$$

ou seja, cálculo da probabilidade dita *a posteriori* é proporcional à amostra X e ao valor fixo atual pertencente a X.

Assim, tem-se a reputação atualizada igual ao resultado da distribuição *a posteriori*, que é calculado utilizando a reputação atual (distribuição *a priori*) e o novo valor de confiança fornecido. A vantagem dessa técnica é que ela possui um embasamento teórico fundamentado em teorema e modelos estatísticos. A desvantagem é dificuldade que o usuário terá de compreender com é feito o cálculo da confiança.

Outras formas de se calcular confiança e reputação incluem lógica difusa e modelos baseados em fluxos. Lógica difusa prevê regras para o raciocínio difuso com medidas que contemplam valores intermediários em verdadeiro e falso, ou confiável e não confiável. Trabalhos como o de Song e Hwang [9], Quillinan et al [22] e de Sabater e Sierra [38] se encaixam nesse modelo.

São chamados de modelos de fluxo aqueles modelos que calculam confiança ou reputação por iterações transitivas através de laços ou longas cadeias arbitrárias [29]. Alguns modelos de fluxo assumem um peso constante para a confiança ou reputação e esse valor pode ser redistribuído para toda comunidade. Assim, os participantes só conseguem aumentar sua reputação às custas de outros. Esse é, por exemplo o esquema utilizado pelo algoritmo de PageRank do Google [39]. Outros modelos de fluxo não utilizam um peso constante para definir a reputação. Esse é o caso do EigenTrust [18], que calcula a reputação através de repetidas e iterativas multiplicações e agregações dos valores de confiança através das relações transitivas de toda a comunidade até que esse valor convirja para valores estáveis.

3.1.1 - Exemplos de Cálculo de Confiança

Azzedin e Maheswaran foram importantes difusores da utilização do cálculo de confiança por meio de valores objetivos e sem utilizar lógica difusa [46]. Em [48] e [49] eles utilizaram uma função linear para cálculo da confiança, *T(x,y,t)*, que considera uma função para confiança direta, aquela baseada nas experiências que uma entidade possui sobre o comportamento de outra, e uma função de reputação, que representa a avaliação da comunidade sobre a entidade que se pretende confiar.

$$\Gamma(x, y, t) = w_d * \Theta(x, y, t) + w_r * \Omega(x, y, t) \quad (4)$$

Onde *Wd* e *Wr* são os pesos da confiança direta e da reputação (constantes que somadas resultam 1) e

$$\Theta(x, y, t) = DTT(x, y) * \Upsilon(t - t_{xy}) \quad (5)$$

e

$$\Omega(x, y, t) = \frac{\sum_{z \in \mathcal{D}-x} RTT(z, y) * R(z, y) * \Upsilon(t - t_{zy})}{|\mathcal{D} - x|} \quad (6)$$

onde Y é uma função de depreciação da confiança em função do tempo; *D* é o domínio das entidades; t_{zy} é o tempo (data e hora) da última interação de z com y; DTT e RTT são respectivamente as tabelas de confiança direta e de reputação (*Direct trust table* e *Reputation Trust Table*); e *R(z,y)* ∈ [0,1] e representa a nossa confiança de que não há um complô entre z e y.

O cálculo da reputação do PeerTrust [21] é feito como mostra a equação 7. *T(u)* representa o valor de confiança de *u*; *I(u,v)* denota o número de transações realizadas entre os *peers u* e *v* e *I(u)* o total de transações de *u* com todos os outros *peers*; *p(u,i)* denota outro *peer* participando da *i*ésima transação de *u*; *Cr(v)* representa a credibilidade do feedback de *v*; *TF(u,i)* denota um fator adaptativo do contexto da transação de *u* na *i*ésima transação; *CF(u)* denota o fator adaptativo do contexto da comunidade e alfa e beta representam o fatores de peso normalizados para a avaliação coletiva dos *peers* e do fator de contexto da comunidade.

$$T(u) = \alpha * \sum_{i=1}^{I(u)} S(u, i) * Cr(p(u, i)) * TF(u, i) + \beta * CF(u) \quad (7)$$

Equação do cálculo de confiança do PeerTrust

3.2 - MODELO DE SISTEMAS DE REPUAÇÕES

Grades computacionais são baseadas em computação distribuída. Devido a essa natureza das grades, uma importante característica a ser verificada nos mecanismos de gerência de confiança é se o modelo utilizado é centralizado ou descentralizado. Modelos centralizados possuem a desvantagem de possuirem um único ponto de falha. Por outro lado, modelos distribuídos implicam em maior complexidade na administração dos valores de confiança, na comunicação e na segurança das informações que trafegam.

3.3 - Centralizado

Nos modelos de reputação de arquitetura de rede centralizada, os valores de confiança que uma entidade possui sobre outra com que teve interação direta são enviadas a um centro de reputação ou a um gerente de confiança. O centro de reputação, que obteve as avaliações de diversos participantes do domínio sobre determinado participante, calcula o valor da reputação e o disponibiliza para consulta para as entidades interessadas.

Com base no valor de confiança fornecido pelo centro de reputação e nas suas próprias informações sobre interações passadas, o participante decide se deve ou não realizar uma transação, prover um serviço ou utilizar um recurso de outra entidade.

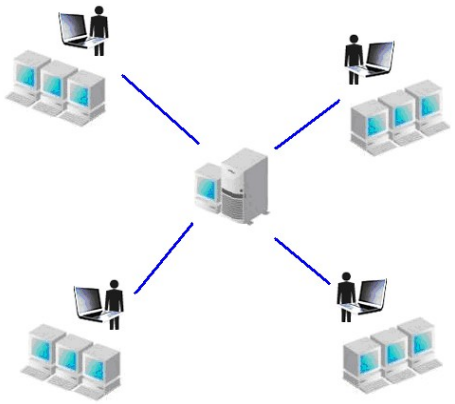

Figura 3 - Modelo centralizado

Na figura 3, as linhas significam que há comunicação e troca de informações. Após cada cooperação, nós usuários e provedores de recursos informam o valor de confiança que possuem um pelo outro para o centro de reputação. O centro, por sua vez, calcula, mantém, disponibiliza e atualiza constantemente o valor da reputação para os participantes da grade.

Nessa abordagem, o gerente de confiança é composto por um só componente com partes não autônomas. Por possuir apenas um ponto de controle também possui a desvantagem de possuir apenas um ponto de falha. Além disso, esses modelos também não possuem nenhuma escalabilidade e não são adequados a grandes ambientes, com diferentes domínios administrativos e com muitos usuários e provedores de recursos, pois todo o processamento, armazenamento e distribuição ficam a cargo de um único nó.

Esse é o esquema utilizado, por exemplo, pelos sites de leilão Ebay e Mercado Livre. Após concretizar uma negociação, comprador e vendedor fornecem um *feedback* ao *web site* avaliando a transação como positiva, neutra ou negativa. O cômputo da reputação do usuário é feito pela subtração das transações negativas das positivas.

Apesar da facilidade de compreensão do valor da reputação e das simplicidades próprias dos sistemas centralizados, este modelo de reputação é muito primitivo e tende a desaparecer [29]. É intuitivo que um usuário que possua 100 avaliações positivas e 10 negativas seja menos confiável do que um que possua 90 positivas e uma negativa, mas nesses sistemas, o primeiro usuário apareceria com maior *score* de reputação do que o segundo.

3.4 - Distribuído

Em sistemas de reputação distribuídos, não há nenhum centro de reputação para enviar avaliações ou obter o valor da reputação e nem nenhuma função centralizada. Nesses sistemas, todo nó é provedor e usuário do sistema de confiança.

Cada nó armazena suas experiências passadas das relações diretas estabelecidas com outros nós e antes de estabelecer uma relação de confiança pode consultar outros nós sobre o valor da reputação da entidade na qual se pretende confiar.

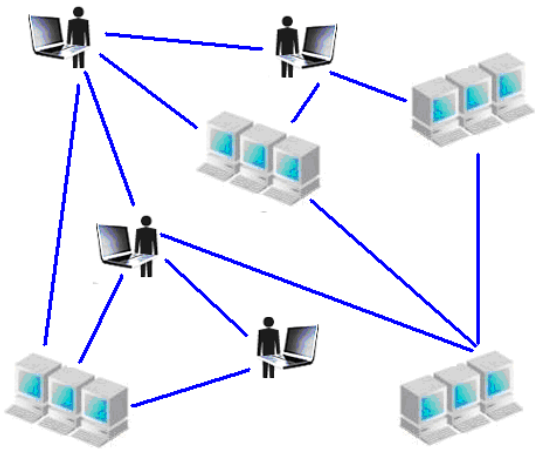

Figura 4 - Modelo Distribuído

Esse é tipicamente o modelo utilizado para gerenciar confiança em redes P2P. Devido ao fato de poder haver uma infinidade de nós, em ambientes distribuídos não há um valor de reputação global para um nó específico. Ao invés disso, o valor global da reputação é baseado nas avaliações dos nós vizinhos.

Em grades computacionais, essa abordagem pode esconder o verdadeiro valor de confiança de usuário. Por exemplo, um usuário pode ser extremamente honesto e possuir níveis altos de confiança em seu domínio, porém pode abusar e utilizar de forma incorreta os recursos de outro domínio. Quando um nó externo ao seu domínio perguntar pelo seu valor de confiança, os nós vizinhos irão responder que ele não é confiável, porém caso a pergunta seja feita no seu domínio, os nós irão responder o contrário e isso implica em dois valores de reputação completamente diferentes para um mesmo nó.

A abordagem utilizada no esquema de avaliação de maturidade do usuário utiliza um modelo distribuído, porém com alguma modificação. O esquema utiliza a adoção de gerentes de confiança como centro de reputação.

Do mesmo modo que pode haver o mesmo tipo de serviço sendo provido por mais de um nó, um mesmo domínio pode ter um ou mais gerentes de confiança de acordo com a sua necessidade. Os usuários e provedores de recursos enviam suas avaliações

para o gerente mais próximo e os gerentes comunicam entre si para compartilhar os valores de reputação dos nós.

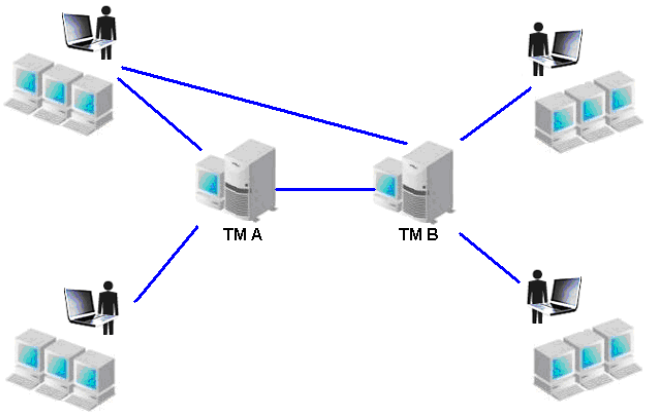

Figura 5 - Modelo utilizado no esquema de avaliação de maturidade do usuário

A Figura 5 mostra a comunicação entre os gerentes de confiança TM-A e TM-B de um mesmo domínio e a comunicação entre nós e gerentes, para enviar avaliações ou obter valores de reputação. Um mesmo nó pode informar a avaliação de confiança sobre a utilização ou provimento do recurso a gerentes diferentes em diferentes interações.

A utilização de diversos gerentes de confiança num mesmo domínio torna o ambiente tão desejado para sistemas pequenos quanto para grandes organizações virtuais, devido a sua escalabilidade.

4 - AVALIAÇÃO DE CONFIANÇA BASEADA NA MATURIDADE DO USUÁRIO

Administradores podem gastar muito tempo para configurar permissões para cada usuário não pertencente ao seu domínio. Para isso, comumente é aplicado uma política para aceitar todos (*approve all*) os pedidos de usuários de um determinado domínio ou negar todos (*reject all*) até que o administrador possua informações suficientes sobre o usuário para liberar o recurso para ele.

Muito desse tempo pode ser economizado se gerência de confiança for utilizada entre o administrador e os usuários da grade. Com esse intuito é que a métrica baseada na avaliação de maturidade do usuário para medir níveis de confiança e o modelo de gerência são propostos, isto é, para atuar entre as tomadas de decisão do administrador do domínio e as requisições dos participantes da grade.

A métrica faz alusão à política de crescimento de um funcionário em uma empresa. Em uma empresa, funcionários que ocupam cargos que requerem menos escolaridade tais como faxineiros e copeiros não têm os mesmos privilégios que um gerente de um setor de produção ou um diretor de alto escalão. Da mesma forma, tais empregados não têm aumento salarial igual ao de seu chefe.

No contexto da proposta, cada usuário possui um grupo e cada grupo possui uma linha de progressão de confiança baseada no nível de maturidade do usuário. O nível de confiança do usuário não ultrapassa um limite máximo pré-estabelecido, chamado de amplitude de confiança.

Ainda utilizando a metáfora dos cargos, o maior salário que um empregado pode receber equivale ao nível máximo de confiança que um usuário pode ter, ou à totalidade de sua amplitude de confiança. Dessa forma, utiliza-se esse nível de modo que um usuário com pouca maturidade, ou de cargo com menos privilégios, fique vetado de utilizar recursos críticos ou recursos não autorizados ao seu grupo.

Em um sistema local, o administrador da grade cadastra os usuários em grupos de forma gradativa de acordo com os recursos que ele queira disponibilizar a cada um deles e as tomadas de decisão passam a poder ser feitas com bases nas permissões do grupo. Caso o usuário seja 100% confiável, ele poderá utilizar todos os recursos

disponíveis para seu grupo e o gerente de confiança o recomendará com nível de confiança máximo.

Considerando uma organização virtual, usuários provenientes de outros domínios administrativos são tratados de forma diferente. Cada domínio externo é associado a um grupo que possui cadastros dos recursos e serviços a ele disponibilizados. Assim cada visitante possui um nível máximo de confiança local de acordo com o domínio administrativo de onde ele provém. Visitantes oriundos de domínios administrativos desconhecidos são tratados em um grupo padrão o qual pode ter algum acesso à grade ou simplesmente serem descartados, considerando que tais usuários não fazem parte da organização virtual.

A interação entre domínios fica a cargo do gerente de confiança. Um gerente de confiança de um domínio possui o nível de confiança de seus usuários e fornece tal informação quando solicitado aos gerentes de outros domínios e aos usuários que quiserem ter informações sobre a reputação do provedor do recurso e vice-versa. Além disso, caso o usuário abuse ou faça mau uso do recurso disponibilizado a ele em outro domínio, seu gerente será alertado para atualizar o nível de confiança do seu usuário. O mesmo vale para um serviço não prestado dentro do contrato estabelecido entre as partes.

É através do gerente de confiança que se obtém a primeira análise do comportamento do usuário proveniente de um domínio externo, ou seja, o nível de confiança daquele usuário no seu domínio de origem. A avaliação do gerente do domínio externo é utilizada em conjunto com a avaliação local e é considerada de acordo com a confiança que um domínio possui sobre o outro.

O que determina o grau de confiança entre os domínios é o comportamento dos usuários em domínios externos e a validação da recomendação feita pelo gerente. Por exemplo, o gerente A do domínio A solicitou ao gerente B do domínio B o nível de confiança que o usuário b1 possui em seu domínio. Porem, o domínio A não confia integralmente nas recomendações feitas pelo gerente do domínio B, por ter havido má utilização do recurso por um usuário que foi recomendado em interações passadas. Com base nesse histórico, o gerente A é capaz de decidir quanto ele confia nas recomendações feitas pelo gerente B, gerando assim um ciclo virtuoso de confiança. Então, conclui-se que o que determina o nível de confiança dos gerentes é histórico de

suas recomendações, ou seja, a reputação do gerente é medida com base nas boas e nas más recomendações.

A adoção de confiança entre gerentes inibe más recomendações de usuários e, por conseguinte, encoraja punições locais ao usuário que abusou ou fez mau uso do recurso externo, ou seja, quanto melhor o comportamento dos usuários de um domínio A externamente, melhor será a reputação de A perante os outros domínios.

A avaliação da maturidade do usuário é baseada num *score* obtido através da análise de critérios precisos, que se seguem:

- **Histórico de utilização dos recursos**: Cada vez que o usuário utiliza um recurso de forma correta, ele recebe pontos e cada vez que ele abusa do recurso ou tenta utilizá-lo de forma incorreta ou não prevista perde pontos, não podendo ultrapassar um limite máximo nem possuir pontuação negativa;
- **Assiduidade de utilização de recursos:** Usuários que utilizam os recursos com mais freqüência tem seu *score* aumentando mais rapidamente. O objetivo desse critério é determinar a porção de crescimento descrita no item anterior. Por exemplo, caso usuário esteja entre os 10% dos usuários que mais utilizam os serviços da grade de forma correta, a pontuação obtida para crescimento por antiguidade é aceita integramente. Caso esteja entre os 10% e os 40% desses usuários, a pontuação é aceita parcialmente com um desconto pré-determinado pelo administrador da grade.
- **Antiguidade**, ou tempo que usuário pertence/visita à grade: Os usuários têm seu nível máximo de confiança limitado por esse critério, para que um novato não tenha todos os privilégios. Esse critério deve ser previamente configurado pelo administrador da grade de modo a estipular períodos de crescimento do nível de confiança para que o usuário há mais tempo na grade possa conseguir acesso a todos os recursos.
- **Avaliação do usuário pelo administrador:** Esse critério não deve ser obrigatório para não exigir interação do administrador no processo de avaliação, mas pode ser utilizado como forma de atribuir alguma penalidade ou prêmio ao usuário.

- **Fator de ajuste do grupo**. Esse valor reflete a porção inicial de confiança que um usuário novato possui na grade.

O histórico de utilização de recursos deve ser limitado há um determinado tempo no passado, isto é, comportamentos mais antigos que uma data específica devem ser desconsiderados, ou seja, comportamentos recentes devem possuir maior peso na avaliação do que comportamentos mais antigos. Portanto, o histórico é delimitado por um período máximo passado, chamado de período de avaliação, onde interações anteriores a esse período não tem valor para a avaliação de maturidade.

Para ter a reavaliação da maturidade feita pelo gerente, o usuário precisa de uma quantidade mínima de pontos durante o período de avaliação. Além disso, é necessário que o usuário possua a antiguidade prevista para aquele nível de maturidade. Por exemplo, para aspirar a primeira progressão e possuir os direitos e privilégios especificados para o seu grupo no segundo nível de maturidade o usuário precisa ter no mínimo um determinado tempo T de antiguidade, ou seja, ele deve pertencer a grade há no mínimo T.

Para manter-se no segundo nível, o usuário agora precisa possuir em seu período de avaliação tantos pontos quanto os necessários para a progressão. Por exemplo, para o usuário obter a primeira progressão, foram necessárias 50 pontos e pertencer à grade há pelo menos T unidades de tempo sendo assim, o usuário precisa manter ao menos 50 pontos no últimos T tempos mais recentes. Dessa forma, usuários que utilizam pouco ou esporadicamente não conseguem alcançar níveis de confiança mais elevados. Pode-se comparar esses usuários a empregados preguiçosos, que trabalham pouco ou não procuram se qualificar.

A assiduidade de utilização de recursos é utilizada para acelerar a progressão da maturidade do usuário. Como uma forma de beneficiar os usuários mais ativos e que por sua vez, avaliam e fornecem mais informações sobre os recursos que utilizam e também são mais avaliados, o administrador pode prever pesos diferentes para a atribuição de pontos para os usuários mais assíduos.

Ao contrário do que alguns autores dizem, é importante considerar a antiguidade do usuário quando se trata de confiança e reputação. Retomando a definição inicial, confiança é uma medida subjetiva e possui características inerentes ao comportamento do usuário. Os modelos computacionais de avaliação de confiança devem se aproximar

ao máximo do sentimento e de relações de confiança da forma como costumamos considerar no dia a dia. Modelos como [20] e [50] consideram uma função de decaimento do valor da confiança com o passar do tempo. Dessa forma os tais modelos impõem a constante utilização de recursos e assim estimula as organizações a penalizar seus usuários.

Em continuidade ao raciocínio anterior, é importante considerar a antiguidade para aproximar o modelo da realidade devido ao caráter humano do valor de confiança. Um empregador não confia integralmente e nem contrata de forma permanente os serviços de uma pessoa que ele acabou de conhecer. Por melhor que tenham sido suas recomendações, o primeiro contrato de trabalho entre as partes é sempre um contrato de experiência. Esse é o fator que deseja-se incluir ao considerar a antiguidade do usuário. A antiguidade limita a progressão da maturidade independente da quantidade de interações, *score* ou recursos utilizados, isto é, por mais ativo e pontuado que o usuário seja, se ele não possuir a antiguidade necessária ele não consegue alcançar níveis de confiança mais elevados.

Como forma de flexibilizar as progressões, o que chamamos de avaliação do usuário pelo administrador funciona como uma constante a ser somada ou subtraída da pontuação do usuário. Assim o modelo proporciona uma forma de abarcar políticas que podem definir, por exemplo, bonificações para usuários e cuidar de casos excepcionais que possam ocorrer.

Discutidos os fatores que influenciam diretamente no valor de confiança, para o cálculo do referido valor quando da avaliação de maturidade do usuário pelo gerente de confiança de seu domínio, estabeleceu-se as equações descritas a seguir.

Para calcular a quantidade pontos que irá indicar o nível de maturidade do usuário utilizamos a avaliação do administrado, o fator de ajuste do grupo e as interações positivas do usuário. As interações positivas de um usuário *u* são todas as interações de *u* que foram informadas como corretas e não maliciosas ao Gerente de Confiança pelos diversos provedores de recurso com os quais *u* interatuou. Assim, temos P_u com o total de pontos que determinam o nível de maturidade do usuário *u* e é obtido pelo menor valor entre T_u e $MaxGrp_i$.

$$P_u = \min (T_u, MaxGrp_i) \quad (8)$$

$MaxGrp_i$ é máximo de pontos que os usuários do grupo *i* podem alcançar. T_u é o total de pontos obtidos através da soma dos valores de Adm(*u*), $Ajus_i$, e o menor valor entre a pontuação de obtida pelas interações positivas de *u*, representado na equação 9 por I_u , e o máximo de pontos permitido para a antiguidade dos usuário do grupo *i*, representado por Ant_i. Adm(*u*) é a avaliação do administrador do domínio feita sobre *u*. $Ajus_i$ é o fator de ajuste de pontos do grupo *i* e determina a porção inicial de confiança dos usuários deste grupo.

$$T_u = Adm(u) + Ajus_i + \min(I_u, Ant_i) \qquad (9)$$

Para o cálculo da pontuação obtida pelas interações positivas, I_u, considera-se a quantidade de interações positivas de *u* e a assiduidade de utilização dos recursos de *u*. Então,

$$I_u = NI_u * As_u \qquad (10)$$

onde NI_u é o número de interações positivas de *u* e As_u a assiduidade de *u*, onde $0 \leq As \leq 1$.

Com a determinação da pontuação, o administrador do domínio pode compor intervalos de pontuação para estabelecer a amplitude de confiança para os diversos grupos de usuários.

Para usuários provenientes de domínios administrativos externos computa-se ainda a recomendação do gerente externo de modo que ela delimite o máximo de pontos que tais usuários podem alcançar. A equação 11 apresenta tal definição:

$$MaxPts_e = Rec(v) * T(TM_E) * (MaxGrp_e - Ajus_e) + Ajus_e \qquad (11)$$

O máximo de pontos que um usuário *v* de um domínio externo E pode alcançar é determinado pelo máximo de pontos que os usuários do grupo *e* podem alcançar, $MaxPts_e$. $MaxPts_e$ é dado pela multiplicação da recomendação que o gerente de confiança de *v* fez sobre ele, representado na equação 11 por Rec(v), e a confiança que o

gerente de confiança local possui sobre o gerente externo que fez a recomendação, representada por T(TM_E), aplicada sobre o intervalo mínimo e máximo de pontos do grupo *e*, onde $0 \leq \text{Rec}(v) \leq 1$ e $0 \leq \text{T}(TM_E) \leq 1$.

4.1 - Interação Entre Gerentes

Para gerenciar os valores de confiança, é proposta uma forma de interação entre gerentes de confiança com para permitir a propagação e atualização dos níveis de confiança dos gerentes.

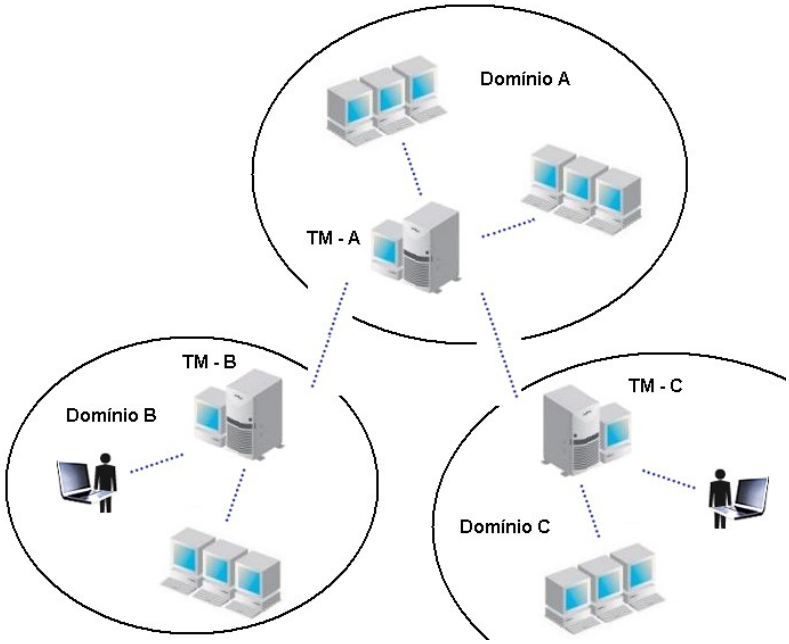

Figura 6 - Interação entre gerentes de confiança.

Os gerentes de confiança atuam como provedores de serviços na grade. Através do serviço de descoberta de recursos, os gerentes podem trocar informações entre si. Num mesmo domínio, a existência de mais de um gerente de confiança funciona como replicação dos valores de confiança de seus usuários provendo escalabilidade e balanceamento de carga e evita problemas como a queda do serviço e suprindo, por exemplo, possíveis falhas de comunicação que possam ocorrer em uma área da grade.

Assim, por haver a possibilidade de um domínio possuir diversos gerentes, os valores de confiança dos gerentes devem ser sincronizados periodicamente.

A figura 6 mostra a interação entre os gerentes de confiança (TM – *Trust Manager*) de três domínios A, B e C. Cada gerente possui em uma tabela o nível de confiança que um gerente tem em outro. Dessa forma, um gerente A pode julgar quanto ele deve confiar nas informações e recomendações feitas pelo gerente B com base no nível de confiança que os outros gerentes conhecidos possuem no gerente B e com base nas informações de recomendações passadas que o gerente B fez ao A.

A atualização dos valores da tabela de confiança entre gerentes conhecidos é feita através da obtenção e troca dessas tabelas com outros gerentes, gerando-se assim, uma nova tabela com a média dos valores recebidos e seus próprios. A atualização da tabela de um gerente A, por exemplo, pode ser feita sempre que um usuário de um domínio externo, E, requisitar um recurso ou serviço ou em intervalos de tempo pré-determinados. Dessa forma, passa a existir uma forma de qualificar as recomendações feitas pelo gerente E, isto é, com base nos níveis de confiança que os outros gerentes possuem sobre o gerente de E é possível calcular quanto se deve confiar nas recomendações feitas por ele.

Além da tabela de confiança entre gerentes, cada gerente mantém também o nível de maturidade de cada usuário pertencente ao seu domínio. Nós usuários e provedores de recursos pertencentes a um mesmo domínio interagem com o gerente de confiança informando o sucesso ou fracasso na execução das tarefas, a competência do usuário em produzir códigos seguros e que não prejudiquem o desempenho da grade e se utilizaram os recursos da forma prevista e contratada.

5 - EXPERIMENTOS E RESULTADOS

A tabela 1 expressa a relação entre recursos disponíveis e o nível de maturidade dos usuários. Usuários com maturidade nível 1 podem utilizar apenas recursos de nível 1; usuários do grupo 2 podem utilizar recursos do nível 1 e 2 e assim sucessivamente conforme a tabela 1.

<table>
<tr><th>Recursos</th><th>Recursos nível 1</th><th>Recursos nível 2</th><th>Recursos nível 3</th><th>Recursos nível 4</th></tr>
<tr><td rowspan="4">Nível de Maturidade</td><td>Nível 1</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Nível 2</td><td></td><td></td></tr>
<tr><td colspan="3">Nível 3</td><td></td></tr>
<tr><td colspan="4">Nível 4</td></tr>
</table>

Tabela 1 – Recursos e para acesso a recursos

Para simular diversas interações e avaliações de maturidade, estipulou-se que as reavaliações dos níveis de maturidade dos usuários serão realizadas aproximadamente a cada 30 segundos. O período de avaliação é de 120 segundos, ou seja, interações positivas ocorridas ha mais de 120 segundos do momento de avaliação serão desconsideradas. Para todos os grupos, a antiguidade limita em 5 a cada 30 segundos os pontos de interações positivas, ou seja, caso o usuário possua 60 segundos de antiguidade e tenha conseguido 15 pontos de interações positivas, passará a ter 10 pontos. O fator de ajuste do grupo e máximo de pontos do grupo, que irão determinar a amplitude de confiança, e estão dispostos na tabela 2.

Grupo	Fator de ajuste do grupo	Máximo
GRUPO 1	10	∞
GRUPO 2	20	∞
GRUPO 3	30	∞

Tabela 2 – Fator de ajuste do grupo e máximo de pontos do grupo.

A pontuação mínima necessária obtida pelas interações positivas para que o usuário tenha a reavaliação do nível de maturidade é 10. Os intervalos de pontuação e antiguidade necessários para cada nível de maturidade utilizados nas simulações são os que seguem na tabela 3.

Nível de Maturidade	Pontos necessários	Antiguidade necessária
Nível 1	0	0 segundos
Nível 2	20	50 segundos
Nível 3	40	200 segundos
Nível 4	60	500 segundos
Nível 5	100 ou mais	Mais de 800 segundos

Tabela 3 – Fator de ajuste do grupo e máximo de pontos do grupo.

O experimento foi realizado com diversas simulações de comportamento de usuários para demonstrar a evolução do nível de maturidade. A tabela 4 apresenta a massa de dados gerada aleatoriamente para 3 usuários com comportamentos diferentes. O usuário U_1 pertence ao grupo 1, não possui avaliação do administrador e têm, em média, 80% de suas interações informadas como positivas ao gerente de confiança. O usuário U_2, pertence ao grupo 2, também não possui avaliação do administrador e têm aproximadamente 50% de suas interações informadas como positivas ao gerente de confiança. O usuário U_3 pertence ao grupo 3, possui 10 pontos de avaliação do administrador e têm por volta 90% de suas interações informadas como positivas ao gerente de confiança. A assiduidade para todos os usuários é 1. O Número de interações exposto na segunda coluna da tabela 4 é a quantidade de interações, positivas ou não, desde a última reavaliação do nível de maturidade.

Tempo da avaliação de maturidade	Número de interações			Pontuação por interações positivas (I_u)			Pontuação total (P_u)			Nível de maturidade		
	U_1	U_2	U_3	U_1	U_2	U_3	U_1	U_2	U_3	U_1	U_2	U_3
30s	8	11	10	6	7	9	15	11	15	1	1	1
60s	10	10	11	14	15	18	20	17	20	2	1	2
90s	13	9	14	25	21	30	25	25	25	2	2	2
120s	15	9	13	32	24	39	30	30	30	2	2	2

150s	14	9	12	40	21	42	35	34	35	2	2	2
180s	14	9	10	43	19	40	40	31	40	2	2	2
210s	12	12	10	40	18	39	45	29	45	3	2	3
240s	16	11	17	44	19	45	50	28	50	3	2	3
270s	16	10	14	41	23	46	50	29	55	3	2	3
300s	14	19	16	43	28	53	53	33	60	3	2	3
330s	16	21	14	50	34	53	60	38	63	3	2	3
360s	16	19	14	48	41	52	58	44	62	3	3	3
390s	16	29	19	51	51	58	61	51	68	3	3	3
420s	18	30	21	53	57	61	63	61	71	3	3	3
450s	21	30	20	58	64	69	68	67	79	3	3	3
480s	31	30	28	73	64	83	83	74	90	3	3	3
510s	31	30	30	86	57	94	96	74	95	4	4	4
540s	31	30	30	94	50	102	104	67	100	4	4	4
570s	31	30	30	98	51	111	108	60	105	4	4	4
600s	31	30	30	92	51	107	102	61	110	4	4	4
630s	31	30	30	93	57	104	103	61	114	4	4	4
660s	31	30	30	90	60	106	100	67	116	4	4	4
690s	31	30	30	93	57	105	103	70	115	4	4	4
720s	21	30	30	89	56	106	99	67	116	4	4	4
750s	20	30	30	78	58	108	88	66	118	4	4	4
780s	23	30	30	66	60	110	76	68	120	4	4	4
810s	18	30	30	64	54	109	74	70	119	4	4	5
840s	21	30	30	64	56	109	74	64	119	4	4	5
870s	23	30	30	69	50	107	79	66	117	4	4	5
900s	21	30	30	64	46	103	74	60	113	4	4	5
930s	31	30	30	74	52	103	84	56	113	4	3	5
960s	20	30	30	74	50	108	84	62	118	4	4	5
990s	31	30	30	80	50	108	90	60	118	4	4	5
1020s	31	30	30	90	48	110	100	60	120	5	4	5
1050s	31	30	30	89	50	107	99	58	117	4	3	5
1080s	21	30	30	86	56	107	96	60	117	4	4	5
1110s	20	30	30	81	57	110	91	66	120	4	4	5
1140s	21	30	30	72	66	106	82	67	116	4	4	5
1170s	21	30	30	56	67	109	66	76	119	4	4	5
1200s	20	30	30	60	61	107	70	77	117	4	4	5
1230s	20	30	30	56	61	104	66	71	114	4	4	5
1260s	31	30	30	64	58	107	74	71	117	4	4	5
1290s	31	30	21	76	56	98	86	68	108	4	4	5
1320s	30	23	23	86	55	91	96	66	101	4	4	5
1350s	31	29	18	96	56	80	106	65	90	5	4	4
1380s	31	30	16	98	54	67	108	66	77	5	4	4

Tabela 4 – Massa de dados

Podemos notar no usuário U_1 que de 500 a 600s ele possuía os pontos necessários para atingir o nível 5 de maturidade porém, não possuía antiguidade suficiente que, nesse caso, era de 800s.

O gráfico da figura 7 mostra a evolução da pontuação e durante as avaliações de maturidade e denota o comportamento dos usuários 1, 2 e 3.

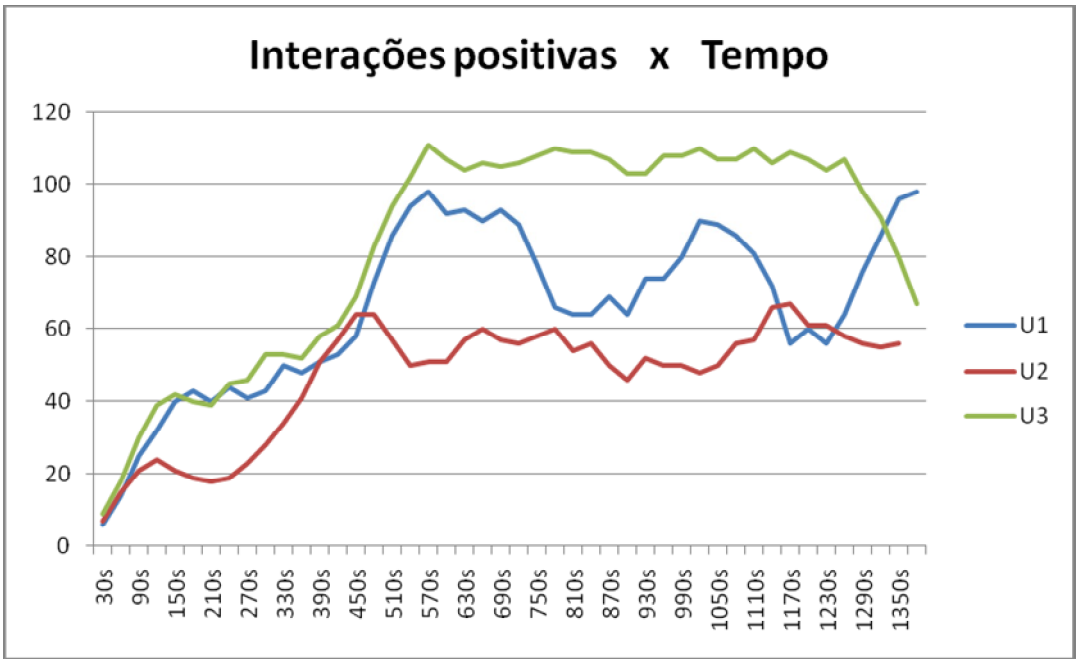

Figura 7 – Interações positivas

Com base na pontuação por interações positivas, a avaliação do administrador e o fator de ajuste do grupo para cada um dos 3 comportamentos, o gráfico da figura 8 demonstra a evolução do nível de maturidade dos usuários 1, 2 e 3.

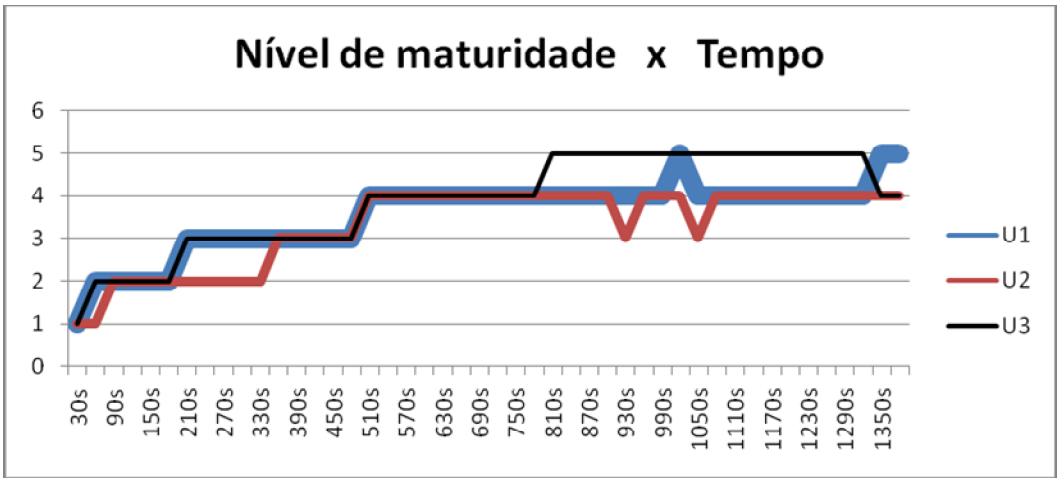

Figura 8 – Evolução do nível de maturidade

Como se pode perceber na figura 7, o usuário U1 inicia com poucas interações e a partir de 500 segundos passa a oscilar a pontuação por interações positivas entre 60 e 100 pontos. Como não há avaliação do administrador e o fator de ajuste do grupo é de apenas 10 pontos, U1 só atinge o nível 5 de maturidade nos dois picos posteriores a 800 segundos. O usuário U2, por manter menos interações positivas, levou mais tempo para obter níveis de maturidades maiores. Já o usuário 3, além de manter a pontuação por interações positivas acima dos 100 pontos por grande tempo, também possuía 10 pontos por avaliação do administrador, além dos 30 pontos de fator de ajuste do grupo, que contribuíram para que ele permanecesse praticamente o tempo posterior a 800 segundos com o mais alto nível de maturidade.

6 - CONCLUSÃO

Este trabalho descreveu onde podem ser obtidas as relações de confiança num curso típico de uma operação em grades; discorreu sobre os tipos de métricas atualmente presentes nas soluções para avaliação de confiança e apresentou uma nova forma para avaliação de confiança que atende diversos requisitos ainda não resolvidos por outras técnicas. Entre eles, um meio para adoção do valor inicial do grau de confiança tanto local quanto no âmbito de uma organização virtual e propôs um modelo de gerência em conjunto com a métrica baseada em reputação que pode ser tão desejado para sistemas pequenos e mais restritos quanto para organizações virtuais por sua característica genérica e por sua escalabilidade.

Também expôs comparou as diversas definições de confiança e reputação, esclarecendo que a medida de reputação é proveniente da opinião de diversos participantes enquanto confiança expressa o "sentimento" direto de uma entidade pela outra e assim contribuindo para o estabelecimento de um senso comum.

Discorreu e exemplificou o as diferentes formas de cálculo de confiança com abordagem específica das características das principais métricas como por valores discretos, por inferência bayesiana, lógica difusa e modelo de fluxos.

Tratou das diferentes abordagens de arquitetura de rede de sistemas de gerência de confiança e propôs uma forma de interação escalável e de baixa complexidade em termos de processamento, armazenamento, disponibilização e atualização dos valores de reputação.

Além disso, apresentou um modelo de gerência que se baseia na maturidade do usuário para avaliar confiança. O modelo de gerência proposto não é atrelado a nenhum *middleware*, nenhuma forma de autenticação, reserva de recursos ou protocolo existente, tornando-o mais flexível e podendo inclusive ser utilizado em conjunto com outras técnicas de avaliação de confiança.

A adoção de gerentes de confiança e o compartilhamento dos valores de reputação dos usuários e o dos próprios gerentes entre si introduzem um novo modelo de gerência visto que eles lidam apenas com confiança, sem fazer alocação ou reserva de recursos, e

considera apenas o comportamento do usuário para fazer recomendações, tanto para outros gerentes quanto para os sistemas subjacentes.

O modelo também utiliza os gerentes de confiança como um serviço provido na grade e assim, pode ser replicado. Por esse motivo, possui uma proteção e um diferencial em relação a sistemas centralizados, os quais possuem um único ponto de falha para comunicação, armazenamento, disponibilização e atualização dos valores de reputação.

A comunidade científica também precisa de estudos sobre o impacto dos sistemas de gerência de confiança em grades computacionais. Na bibliografia referenciada, não encontrou-se nenhum estudo a esse respeito.

Como trabalho futuro, uma implementação acomodando o modelo proposto em ambientes reais de autenticação e reserva de recurso e a comparação da sua eficiência frente aos outros métodos de avaliação de confiança encontrados nas soluções atuais.

REFERÊNCIAS BIBLIOGRÁFICAS

1. D. De Roure, M. A. Baker, N. R. Jennings, and N. R. Shadbolt. *The evolution of the grid*. In F. Berman, A. J. G. Hey, and G. Fox, editors, Grid Computing: Making The Global Infrastructure a Reality, p. 65-100. John Wiley & Sons, 2003

2. Foster, I.; Kesselman, C. *The Grid: Blueprint for a New Computing Infrastructure*. San Francisco, CA, USA: Morgan Kaufmann Publishers, 1999. p. 677.

3. Hanif Durad, M.H. Yuanda Cao. *A vision for the trust managed grid.* In Cluster Computing and the Grid Workshops, Sixth IEEE International Symposium. 2006, Volume 2 p. 11.

4. C. Lin, V. Varadharajan, Y. Wang and V. Pruthi. *Enhancing Grid Security with Trust Management.* In Proceedings of the IEEE International Conference on Services Computing (SCC'04), 2004.

5. M. H. Thompson and M. R., *Security implications of typical grid computing usage scenarios.* International Symposium on High Performance Distributed Computing (HPDC), San Francisco, CA, Aug. 7-9, 2001.

6. Humphrey, M.; Thompson, M.R.; Jackson, K.R.; *Security for Grids.* Proceedings of the IEEE, VOL. 93, NO. 3, 2005.

7. Azzedin, F.; Maheswaran, M.; *Evolving and managing trust in grid computing systems.* Electrical and Computer Engineering, 2002. IEEE CCECE 2002. Canadian Conference. p. 1424 - 1429, vol.3, 2002.

8. L. Hui, P. Qinke, S. Junyi, and H. Baosheng. *A mission-aware behavior trust model for grid computing systems*. International Workshop on Grid and Cooperative Computing (GCC2002), Sanya, China, 2002.

9. Song, S.; Hwang, K.; *Fuzzy trust integration for security enforcement in grid computing.* International Symposium on Network and Parallel Computing (NPC), 2004.

10. M. Blaze, J. Feigenbaum, J. Ioannidis and A. Keromytis. *The KeyNote trust-management version 2*. IETF RFC 2704, 1999.

11. C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas and T. Ylonen. *SPKI certificate theory*. IETF RFC 2693. 1999.

12. L. Ninghui, B.N. Grosof and J. Feigenbaum. *Delegation Logic: A logic-based approach to distributed authorization*. ACM Transaction on Information and System Security (TISSEC), 2003.

13. T. Jim. *SD3: a trust management system with certificate evaluation*. In Proceedings of the IEEE Symposium on Security and Privacy, 2001.

14. L. Ninghui, J.C. Mitchel and W.H. Winsborough. *Design of a role-based trust-management framework*. In Proceedings of the IEEE Symposium on Security and Privacy, pages 114-130, IEEE Computer Society Press, 2002.

15. Lin, C.; Varadharajan, V.; Wang, Y.; Pruthi, V. *Enhancing grid security with trust management*. In proceeding of the IEEE International Conference on Services Computing (SCC), 2004.

16. Silaghi, Gheorghe C.; Arenas, Alvaro E.; Silva, Luis M.; *Reputation-based trust management systems and their applicability to grids.* CoreGRID Technical Report Number TR-0064, 2007.

17. Aberer, K. and Z. Despotovic. *Managing trust in a peer-2-peer information system*. In proceedings of the Tenth International Conference on Information and Knowledge Management (CIKM01). pp. 310–317. URL citeseer.ist.psu.edu/aberer01managing.html, 2001.

18. S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. *The eigentrust algorithm for reputation management in p2p networks*. In Proceedings of the Twelfth International World Wide Web Conference (WWW2003). Budapest, Hungary: ACM Press, May 20-24 2003.

19. Zhang, H., A. Goel et al. *Improving eigenvector-based reputation systems against collusion.* Technical report, Stanford University, Workshop on Algorithms and Models for the Web Graph (WAW), 2004.

20. B. Alunkal, I. Valjkovic, G. von Laszewski, K. Amin. *Reputation based grid resource selection.* In proceedings of the 12th InternationalWorldWideWeb Conference on Workshop on Adaptive Grid Middleware (agridm 2003), 2003.

21. Xiong, L. and L. Liu. *Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities.* IEEE Transactions on Knowledge and Data Engineering, 2004.

22. Quillinan, T.B.; Clayton, B.C.; Foley, S.N.; *GridAdmin: decentralising grid administration using trust management.* Workshop on Parallel and Distributed Computing, 2004 on Third International Symposium on/Algorithms, Models and Tools for Parallel Computing on Heterogeneous Networks, 2004.

23. R. Guha, R. Kumar, P. Raghavan, and A. Tomkins. *Propagation of Trust and Distrust*. In International World Wide Web Conference (WWW04), 2004. URL http://citeseer.ist.psu.edu/guha04propagation.html

24. Walsh, K. and E. Gun Sirer; *Fighting peer-to-peer spam and decoys with object reputation*, In proceedings of the SIGCOMM'05 Conference Workshops, Philadelphia, PA, 2005.

25. Muhammad Hanif Durad, Yuanda Cao. *A Vision for the Trust Managed Grid.* Sixth IEEE International Symposium on Cluster Computing and the Grid Workshops (CCGRIDW'06), p. 34, 2006.

26. Azzedin, F., Maheswaran, M. *Evolving and Managing Trust in Grid Computing Systems.* Conference on Electrical and Computer Engineering, Canada. IEEE Computer Society Press, pp1424–1429, 2002.

27. Christianson B. and Harbison W. S. *Why Isn't Trust Transitive?* in Security Protocols International Workshop, University of Cambridge, 1996.

28. T. Grandison, M. Sloman. *A Survey of Trust in Internet Applications*. IEEE Communications Survey and Tutorials, 3, 2000.

29. Jøsang, Audun; Ismail, Roslan; Boyd, Colin. *A Survey of Trust and Reputation Systems for Online Service Provision.* Disponível on-line em: http://citeseer.ist.psu.edu/738255.html, 2006.

30. Diego Gambetta. *Can We Trust Trust?* In D. Gambetta, editor, Trust: Making and Breaking Cooperative Relations, capítulo13, Basil Blackwell. Oxford, 2000

31. Jøsang, Audun. *An Algebra for Assessing Trust in Certification Chains*. In J. Kochmar (editor), Proceedings of the Network and Distributed Systems Security Symposium (NDSS'99). The Internet Society, 1999.

32. Kini, A. and J. Choobineh. *Trust in Electronic Commerce: Definition and Theoretical Considerations.* 31st Annual Hawaii Int'l. Conf. System Sciences, Hawaii, 1998.

33. T. Dimitrakos. *Towards a formal model of trust in e-commerce.* In proceedings of the AI2001 Workshop on Business Agents and the Semantic Web (BASe WEB), 2001

34. D.H. McKnight, N.L. Chervany. *The Meaning of Trust*. Technical Report MISRC Working Paper Series 96-04, University of Minnesota. Management Information Systems Research Center, 1996.

35. Abrams M. D. *Trusted System Concepts,* in Computers and Security, Joyce M. V., Editor, 1995, p. 45 – 56.

36. Ding Y. and Petersen H. *A new approach for delegation using hierarchical delegation tokens*. University of Technology Chemnitz-Zwickau Department of Computer Science, 1995.

37. Liberty-Alliance. *Liberty Trust Models Guidelines*. Disponível em: HTTP://www.oasis-open.org/committees/download.php/6158/sstc-saml-trustmodels-2.0-draft-01.pdf, 2004.

38. J. Sabater and C. Sierra. *Social regret, a reputation model based on social relations*, SIGecom Exch., vol. 3, no. 1, pp. 44–56, 2002.

39. L. Page, S. Brin, R. Motwani, and T. Winograd. *The PageRank Citation Ranking: Bringing Order to the Web*. Technical report, Stanford Digital Library Technologies Project, 1998.

40. A. Jøsang and R. Ismail. *The Beta Reputation System*. In Proceedings of the 15th Bled Electronic Commerce Conference, June 2002.

41. L. Mui, M. Mohtashemi, and C. Ang. *A Probabilistic Rating Framework for Pervasive Computing Environments*. In Proceedings of the MIT Student Oxygen Workshop (SOW'2001), 2001.

42. L. Mui, M. Mohtashemi, C. Ang, P. Szolovits, and A. Halberstadt. *Ratings in Distributed Systems: A Bayesian Approach*. In Proceedings of the Workshop on Information Technologies and Systems (WITS), 2001

43. L. Mui, M. Mohtashemi, and A. Halberstadt. *A Computational Model of Trust and Reputation*. In Proceedings of the 35th Hawaii International Conference on System Science (HICSS), 2002.

44. A. Withby, A. Jøsang, and J. Indulska. *Filtering Out Unfair Ratings in Bayesian Reputation Systems*. The Icfain Journal of Management Research, 4(2):48-64, 2005.

45. Quercia, Daniele; Hailes, Stephen; Capra, Licia. *B-Trust: Bayesian Trust Framework for Pervasive Computing*. Trust Management, 4th International Conference, iTrust 2006, Pisa, Italy, 2006.

46. Brinklov, Michael; Sharp, Robin. *Incremental Trust in Grid Computing.* Cluster Seventh IEEE International Symposium on Computing and the Grid. CCGRID, May, 2007.

47. A. Abdul-Rahman and S. Hailes. "*Supporting Trust in Virtual Communities*". Proceedings of the Hawaii International Conference on System Sciences, Maui, Hawaii, 2000.

48. F. Azzedin and M. Maheswaran. Integrating trust into grid resource management systems. In Proc. 2002 international Conference on Parallel Processing (ICPP'02), pages 47–54. IEEE Computer Society, 2002.

49. F. Azzedin and M. Maheswaran. Towards trust-aware resource management in grid computing systems. In cc-Grid'02: Proc. 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid, pages 452–457. IEEE Computer Society, 2002.

50. Xinhua, Wang; Xiaolin, Gui; Feifei, Chen; *A Trust and Reputation Model of Grid Resources for Cooperating Application.* First International Conference on Semantics, Knowledge and Grid, 2005. SKG '05. 2005.

51. http://www.websters-online-dictionary.org/

52. Information Technology - Open Systems Interconnection – "*The Directory: Authentication Framework*", ITU-T Recommendation X.509, 1997.

53. R. Housley, W. Polk, W. Ford, and D. Solo, "*Internet X.509 Public Key Infrastructure: Certificate and CRL Profile*", RFC 3280, 2002.

54. MIT Distribution Center for PGP (Pretty Good Privacy) [Online]. Available: http://web.mit.edu/network/pgp.html.

55. Neuman, B. C. and Ts'o, T. "*Kerberos: An Authentication Service for Computer Networks*". IEEE Communications Magazine, 32 (9), 33-88, 1994.

56. http://www.epinions.com

57. http://www.amazon.com

58. http://www.ebay.com

59. http://www.mercadolivre.com.br